FEDERATED DATA INFRASTRUCTURE

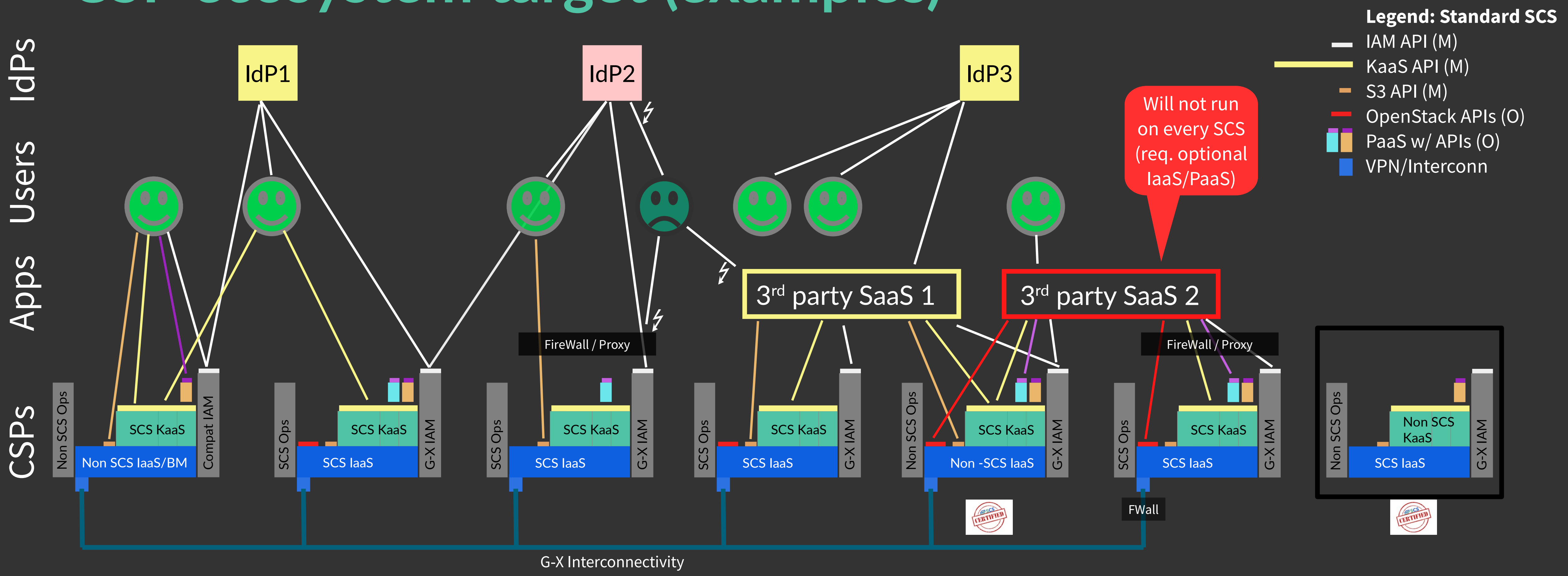
Sovereign Cloud Stack

Back to the original mission: an open cloud operating system

Kurt Garloff
Christian Berendt

Prepared for OpenInfraSummit 2020-10-21

CSP ecosystem target (examples)



Prov1: (public)

Using preex IaaS or BM, not exposing IaaS, Non-Std Ops, Compat IAM

Standard SCS KaaS, S3, PaaS 2

Prov2: (public)

Standard SCS Ops, IaaS (exposed), IAM, KaaS, S3, PaaS 1+2

Prov3: (priv/comm)

Extra protection (limit users/IdPs)

Standard SCS Ops, IaaS (not exposed), IAM, KaaS, S3, PaaS 1

Prov4: (public)

Standard SCS Ops, IaaS (exposed), IAM, KaaS, S3

Prov5: (public)

Non-Standard Ops, IaaS (but certified & exposed as std)

Standard SCS IAM, KaaS, S3, PaaS 1+2

Prov6: (priv/corp)

Extra protection for Interconnect, limited federation

Standard SCS Ops, IaaS (exp), IAM, KaaS, S3, PaaS 1+2

Prov7: (gov/mil)

Air-Gap protected Own KaaS, but compatible (cert)

Still using std SCS Ops, IaaS (not exp), IAM, S3, PaaS 2

SCS project status

Small Project team operational

- Young project, current group came together first in Nov 2019
- Coordinating & orchestrating larger community, bringing IT departments and existing and new providers together
- Funded by SPRIN-D for 2020; funding proposal from OSBA for BMWi in finalization to fund central coordination work; allows contributing companies to build up business models; transfer central work to association/foundation later

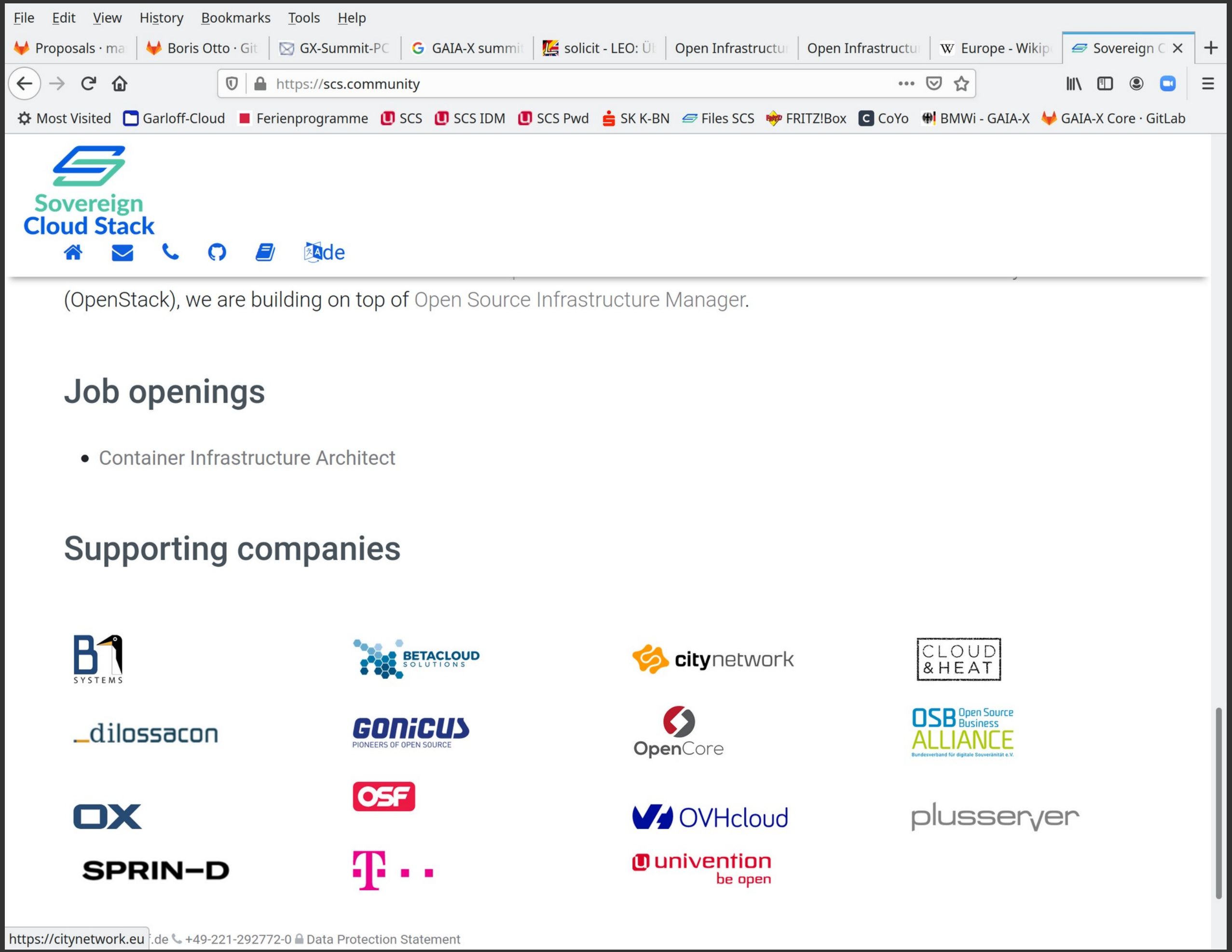
Ecosystem

- Growing number of supporting & contributing partners (OSBA members plus companies from Sweden and France); Continuous SCS installations at 2 (physical) + 7 (virtual) providers
- Trademark, Logo, Web page, github SovereignCloudStack and OSISM
- Part of GAIA-X – SCS is Work Package of GAIA-X. Intense collaboration e.g. w/ IAM
  → Join the GAIA-X summit, Nov 19/20 (virtual event)
- Amazing feedback from many discussions, both industry and public sector
- Public coverage (SPRIN-D, c't, WDR, … see web page)
- Open for more contributions!

Webpage & github

https://scs.community/

github/SovereignCloudStack



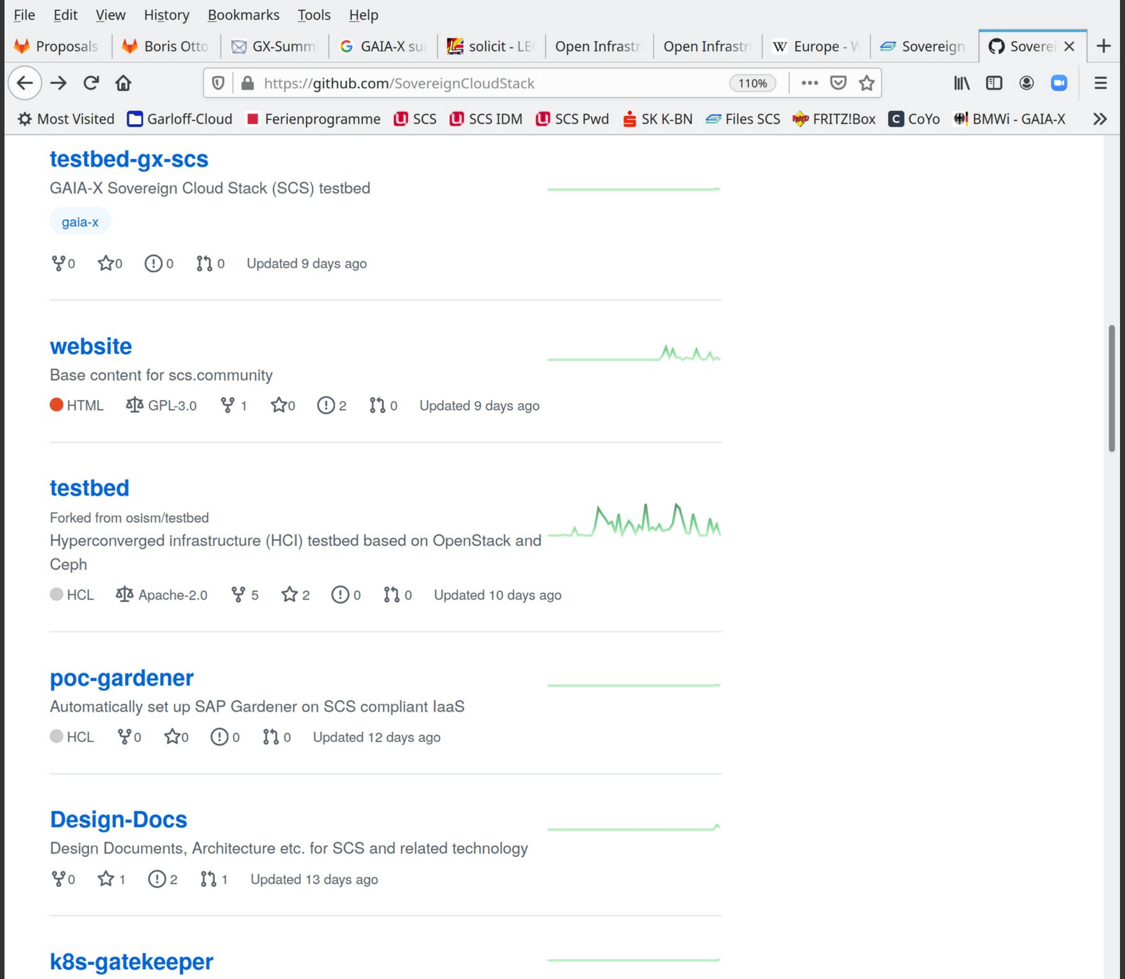
(OpenStack), we are building on top of Open Source Infrastructure Manager.

Job openings

- Container Infrastructure Architect

Supporting companies

.de +49-221-292772-0 Data Protection Statement



testbed-gx-scs

GAIA-X Sovereign Cloud Stack (SCS) testbed

gaia-x

0 ☆0 0 0 Updated 9 days ago

website

Base content for scs.community

● HTML GPL-3.0 1 ☆0 2 0 Updated 9 days ago

testbed

Forked from osism/testbed

Hyperconverged infrastructure (HCI) testbed based on OpenStack and Ceph

● HCL Apache-2.0 5 ☆ 2 0 0 Updated 10 days ago

poc-gardener

Automatically set up SAP Gardener on SCS compliant IaaS

● HCL 0 ☆0 0 0 Updated 12 days ago

Design-Docs

Design Documents, Architecture etc. for SCS and related technology

0 ☆ 1 2 1 Updated 13 days ago

k8s-gatekeeper

SCS technical status (2020-10)

Infra + IaaS + Ops reference implementation pieces operational

- Includes Bare Metal install (MaaS), inventory (Netbox), zabbix, automated containerized install (using ansible) of Manager with Management tooling (ELK, Netdata, ARI, prometheus, skydive, patchman, DB, MsgQ, …) and Hyperconverged Nodes (with KVM, encrypted ceph, OvS/OVN, core OpenStack plus octavia, barbican – vanilla kolla-ansible)
- Virtual deployment ("testbed") can be done on top of another IaaS using terraform – self-hosting (SCS testbed on SCS physical) works of course – ~60 – 90min deployment time.
- Virtual deployment useful for demos, CI testing (smoke-tests, refstack, API monitoring, more TBD …), validating upgrades, exploration, …
- Physical deployments on Bare Metal at two providers (Betacloud (prod), PlusServer)
- Virtual deployment tested on half a dozen providers (Betacloud, PlusServer, CityNetwork, OVH, teuto, OTC – with patches)
- Testbed for GAIA-X ID-Federation using keycloak as ID-Proxy
- Strong SCS standard definitions at IaaS layer (images, flavors, AZ meaning etc.) is WIP

Container layer in development:

- Working with SAP Gardener, kubermatic, Giantswarm, rancher (rke) – challenge is missing standardization for k8s cluster management – MVP planned for Q1/21,
  OpenStack k8s cluster API provider?

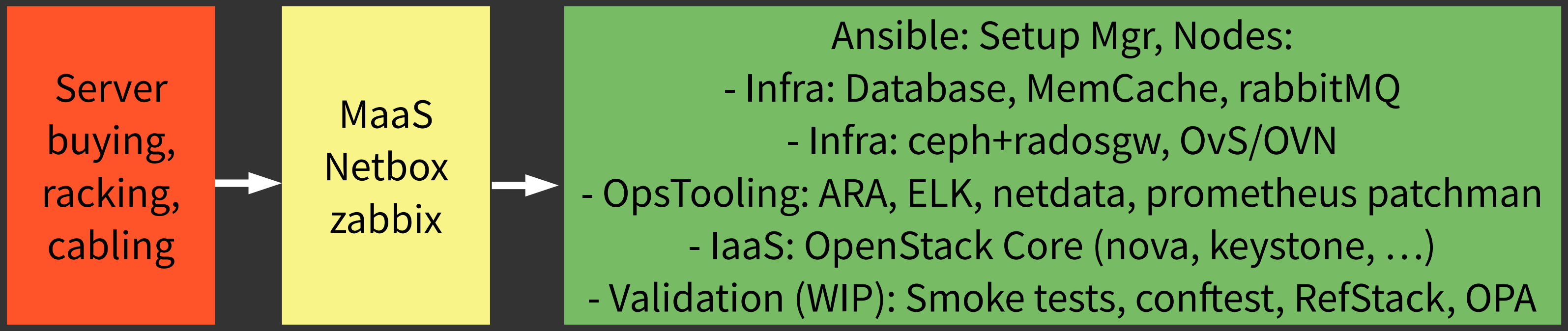
Using testbed framework also for automating other GAIA-X infra, e.g. IAM

Flow of automated deployment (currently covering: Infra, IaaS, Ops)

Physical SCS can of course host virtual SCS
Nested virtualization support recommended

Physical deployment

Production („Live“)



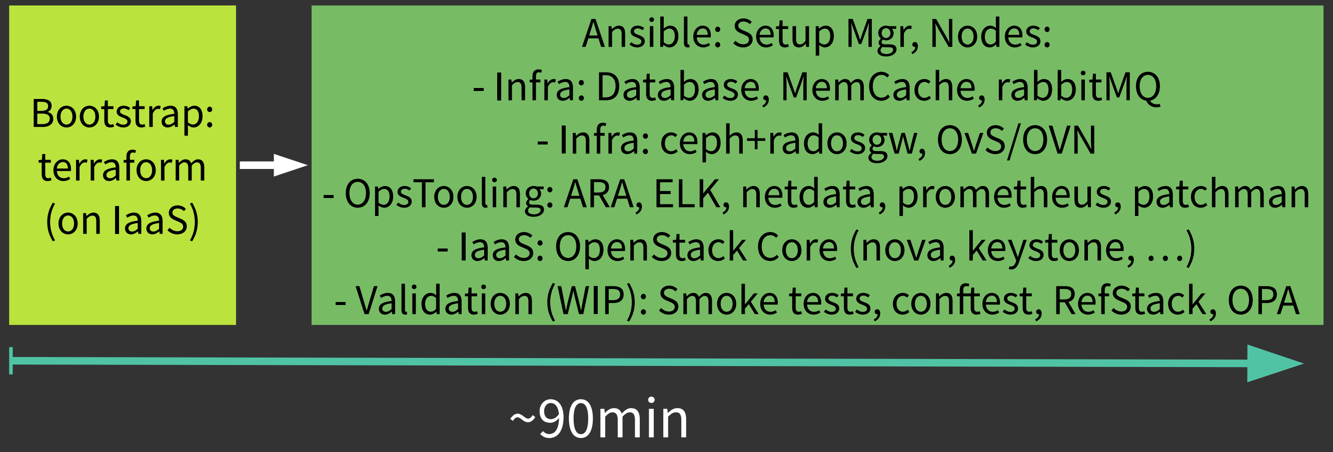
Server buying, racking, cabling

MaaS
Netbox
zabbix

Ansible: Setup Mgr, Nodes:
- Infra: Database, MemCache, rabbitMQ
- Infra: ceph+radosgw, OvS/OVN
- OpsTooling: ARA, ELK, netdata, prometheus patchman
- IaaS: OpenStack Core (nova, keystone, …)
- Validation (WIP): Smoke tests, conftest, RefStack, OPA

Virtual (testbed) deployment

Dev, Testing / CI („Ref/Test“)
Demo, Explore, Debug, …



Bootstrap:
terraform
(on IaaS)

Ansible: Setup Mgr, Nodes:
- Infra: Database, MemCache, rabbitMQ
- Infra: ceph+radosgw, OvS/OVN
- OpsTooling: ARA, ELK, netdata, prometheus, patchman
- IaaS: OpenStack Core (nova, keystone, …)
- Validation (WIP): Smoke tests, conftest, RefStack, OPA

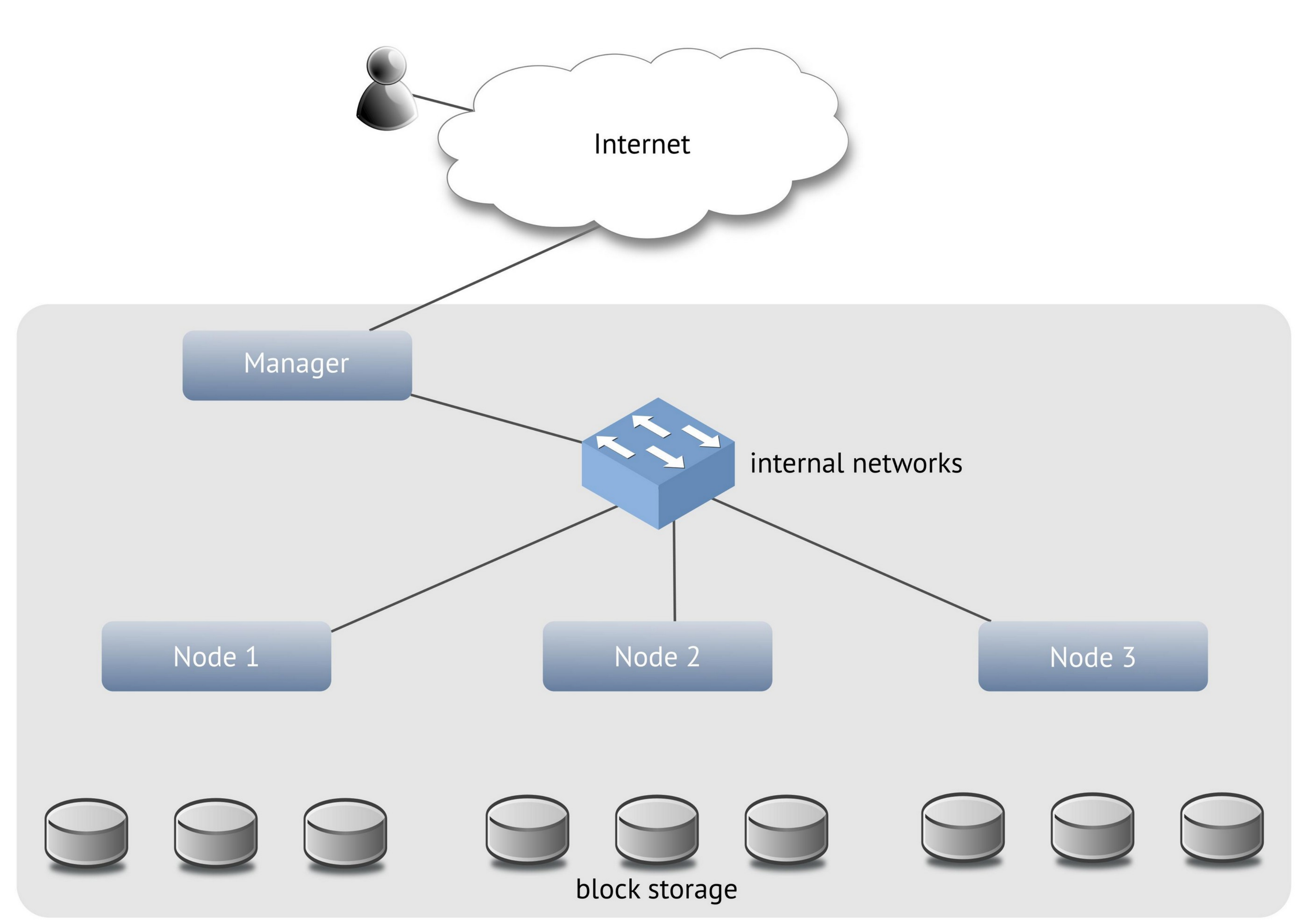
~90min

https://github.com/OSISM https://docs.osism.de/ https://docs.osism.de/testbed/

https://github.com/OSISM/testbed https://github.com/SovereignCloudStack/testbed

Optional Testbed Demo

Minimal testbed setup



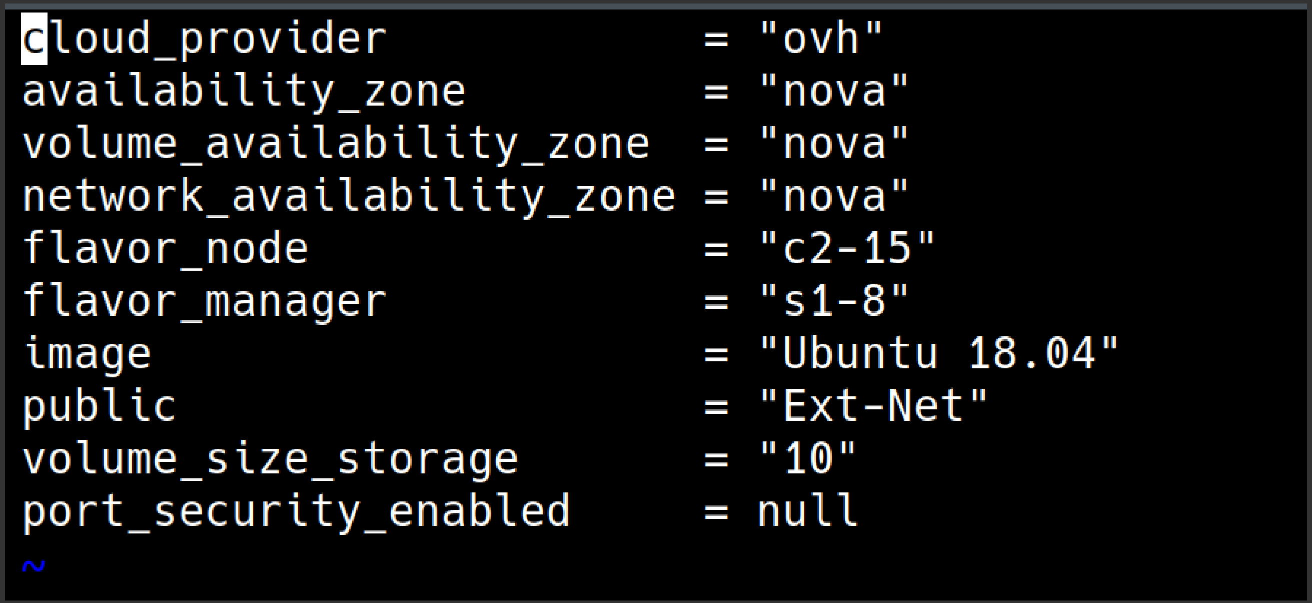
Porting testbed to new cloud

Ensure command line access (openstack client tools) work, install sshuttle, terraform

Ensure sufficient quota (`openstack quota show`): min = 104GiB RAM, 28Cores, 90GiB Storage (+root volumes) on 9 vols, router, 6nets+subnets, 6SGs (50rules), 1FIP, 4 instances

Fill in configuration (`environment-xxx.tfvars`)

- Availability zone
- Flavors (manager, HCI nodes)
- Name of public net
- Image name (Ubuntu 18.04)



```
cloud_provider                = "ovh"
availability_zone             = "nova"
volume_availability_zone      = "nova"
network_availability_zone     = "nova"
flavor_node                   = "c2-15"
flavor_manager                = "s1-8"
image                         = "Ubuntu 18.04"
public                        = "Ext-Net"
volume_size_storage           = "10"
port_security_enabled         = null
~
```

Special work (OVH, OTC) as needed

```
make deploy-openstack watch \
  ENVIRONMENT=xxx
make sshuttle
```

Webinterfaces:
https://docs.osism.de/testbed/usage.html#webinterfaces

Port to terraform libvirt provider WIP

Testbed demo

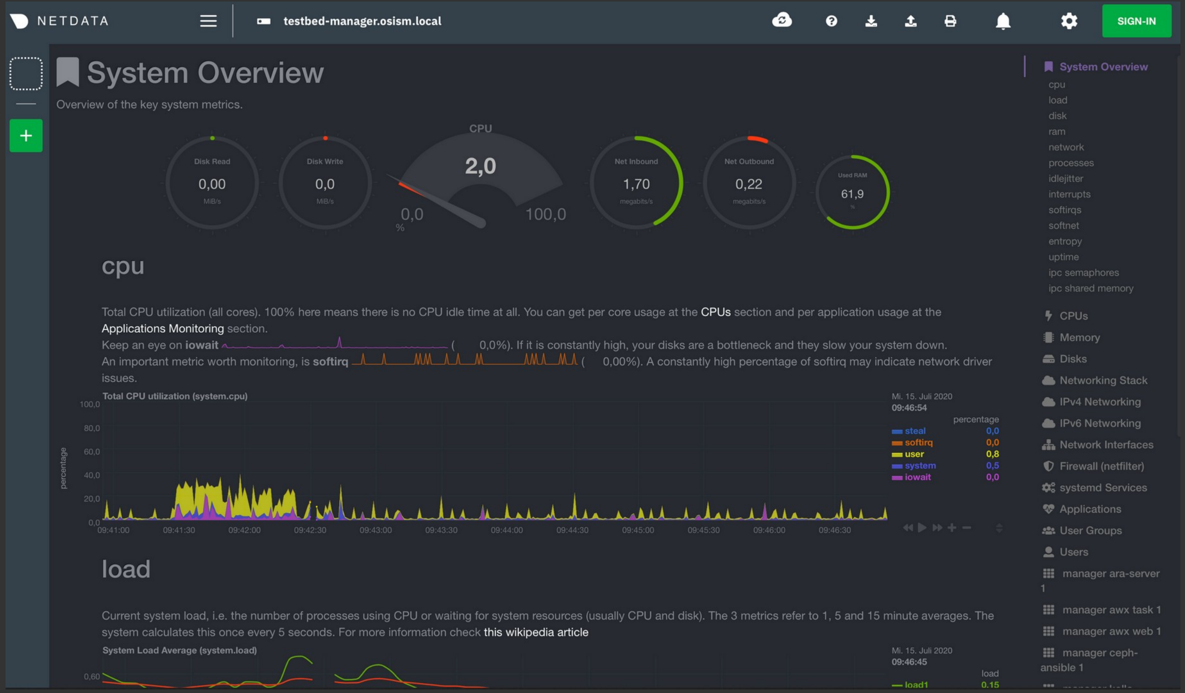
SCS base (OSISM) testbed running on Betacloud, PlusServer, CityCloud, OVH, OTC, C&H

Videos (testbed deployment)

- Start Deployment (terraform, make deploy-openstack watch)
  https://asciinema.org/a/fCxgxV8a5bJMtubw8mBPdtozl
- Ceph & OpenStack deployment
  https://asciinema.org/a/E0dUtNlftLOLZRu6ajawi9lbo
  https://asciinema.org/a/FD90KLmSGp9lWT1jTF6S9yBJj

Web interfaces

- Ceph dashboard
- Cockpit
- netdata
- Skydive
- Patchman
- Kibana
- Horizon
- …



System Overview

Overview of the key system metrics.

cpu

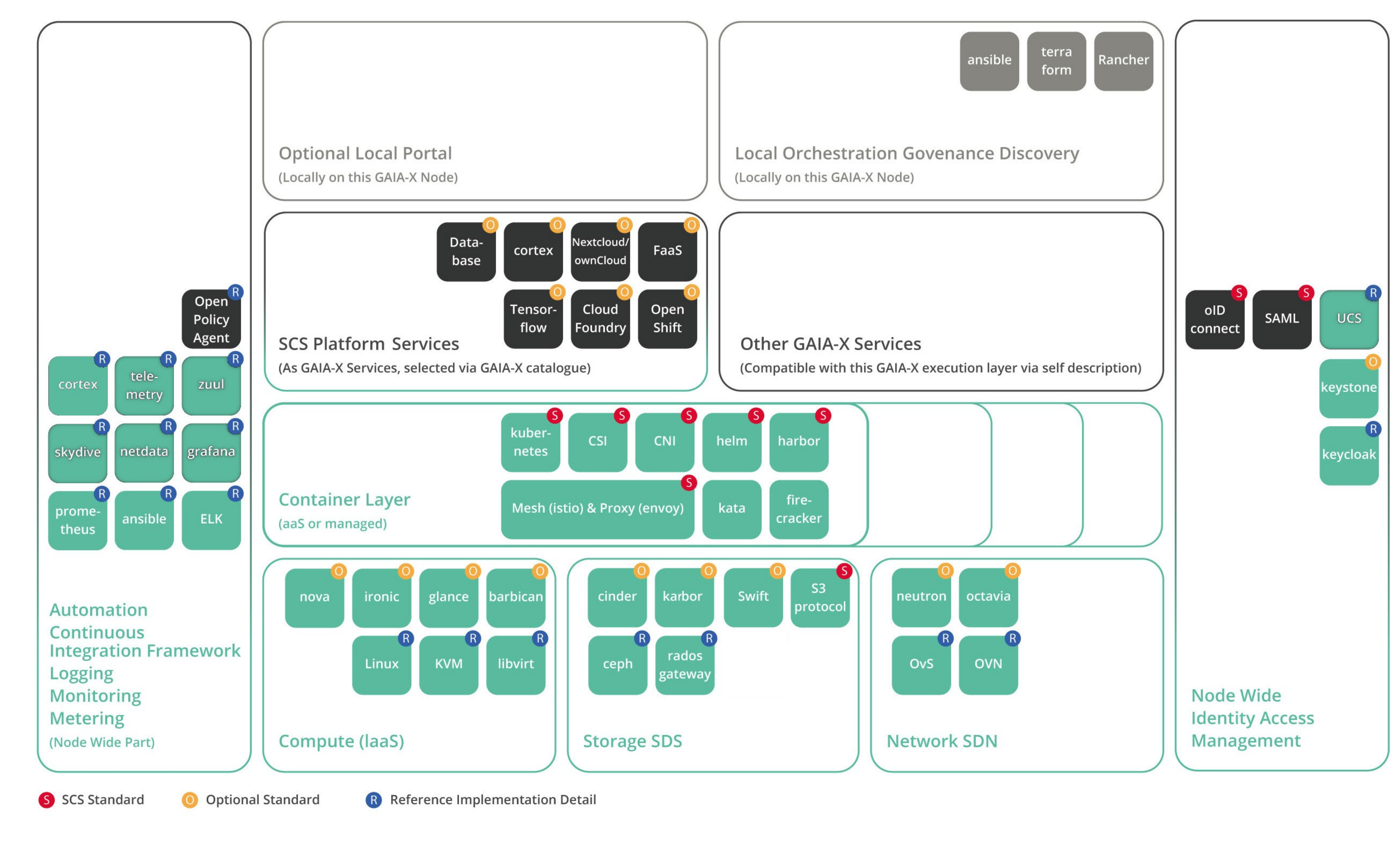
Total CPU utilization (all cores). 100% here means there is no CPU idle time at all. You can get per core usage at the CPUs section and per application usage at the Applications Monitoring section.
Keep an eye on **iowait** (0,0%). If it is constantly high, your disks are a bottleneck and they slow your system down.
An important metric worth monitoring, is **softirq** (0,00%). A constantly high percentage of softirq may indicate network driver issues.

load

Current system load, i.e. the number of processes using CPU or waiting for system resources (usually CPU and disk). The 3 metrics refer to 1, 5 and 15 minute averages. The system calculates this once every 5 seconds. For more information check this wikipedia article

docs

Architecture (current status)



ansible
terra form
Rancher

Optional Local Portal
(Locally on this GAIA-X Node)

Local Orchestration Govenance Discovery
(Locally on this GAIA-X Node)

Data- base O
cortex O
Nextcloud/ ownCloud O
FaaS O
Tensor- flow O
Cloud Foundry O
Open Shift O

SCS Platform Services
(As GAIA-X Services, selected via GAIA-X catalogue)

Other GAIA-X Services
(Compatible with this GAIA-X execution layer via self description)

Open Policy Agent R
cortex R
tele- metry R
zuul R
skydive R
netdata R
grafana R
prome- theus R
ansible R
ELK R

Automation
Continuous Integration Framework
Logging
Monitoring
Metering
(Node Wide Part)

kuber- netes S
CSI S
CNI S
helm S
harbor S
Mesh (istio) & Proxy (envoy) S
kata
fire- cracker

Container Layer
(aaS or managed)

nova O
ironic O
glance O
barbican O
Linux R
KVM R
libvirt R

Compute (IaaS)

cinder O
karbor O
Swift O
S3 protocol S
ceph R
rados gateway R

Storage SDS

neutron O
octavia O
OvS R
OVN R

Network SDN

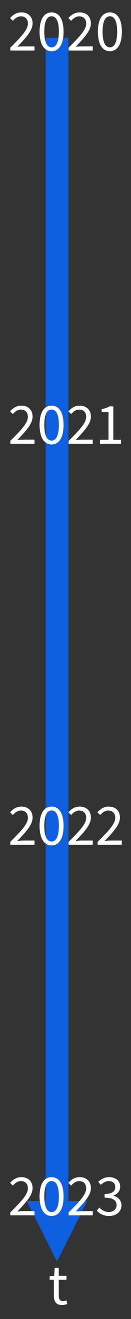
oID connect S
SAML S
UCS R
keystone O
keycloak R

Node Wide Identity Access Management

S SCS Standard
O Optional Standard
R Reference Implementation Detail

Roadmap

Automate deployment for Infra, IaaS, OpsTools √
Resolve k8s aaS automation std challenge (v1 until end of 2020)
Strengthen CI (ongoing)
Implement daily updates for production (v1 in 2020)
Implement OPA policies (v1 in 2020)
Document SCS certification requirements (1H 2021)
Create plan for Security Certifications (BSI, TC, ISO, …)
Start implementing first PaaS services (DB, Big Data, …) (1H2021)
Cloud federation use cases (1H2021)
Automation for SCS certification (2H2022)
Monitoring driven mitigation – remediation workflows (v1 in 2H2021)
Access to acceleration technologies (2H2021)
SDN scalability work (1H2022)
Cross-cloud orchestration & monitoring (1H2022)
Utilization optimizations (2022)
Developer toolchain (starting in 2021)
Simplified stacks for special use cases (2022)
AI supported operations (2023)



WG/WorkPkg in GAIA-X √
Code on github √
Press / WebPage √
GAIA-X AISBL incorp
More virtual SCS deployments
Leverage GAIA-X IAM and Network
Funding

Developer onboarding (ongoing)
Productive use (IaaS)
Sec Certification
SCS foundation/association
Productive use (KaaS)
Partner ecosystem (support, training, …)

Ecosystem growth

EPI collaboration?

PaaS, SaaS

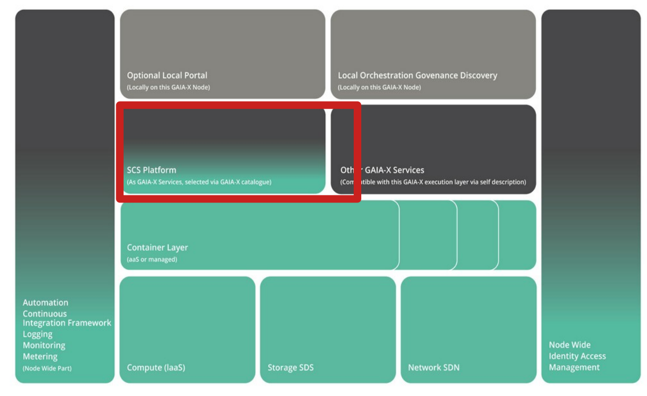
Self-service in own cluster with operator provided repository of curated building blocks

Operator managed shared cluster for higher-level services (PaaS and SaaS)

- Use k8s operators for these
  DB aaS, AI/ML, FaaS, Collaboration, DevStory
- Open Source projects like Stackable, Postgres, Tensorflow, Nextcloud/Owncloud,
  Collabora, OX, CloudFoundry, OpenShift, …
- Developer story
  - Provide tooling for automation (helm, terraform etc.) and CI/CD (zuul, Jenkins, …)
  - Registry and Security scanning tools (harbor, octarine, …)
  - Tracing, auditing, monitoring (cortex)
  - Documentation (Best Practices …)
  - Many more possibilities …
- Be the best platform for GAIA-X federation services
- Be a very good platform for GAIA-X data services (IDSA et.al.)

Status: Concept phase

- Space not yet mapped out completely, some PoCs done (harbor, minio, …)
- Leave space for ecosystem – move up the stack **slowly and predictably**



Optional Local Portal
(Locally on this GAIA-X Node)

Local Orchestration Govenance Discovery
(Locally on this GAIA-X Node)

SCS Platform
(As GAIA-X Services, selected via GAIA-X catalogue)

Other GAIA-X Services
(Compatible with this GAIA-X execution layer via self description)

Container Layer
(aaS or managed)

Automation
Continuous
Integration Framework
Logging
Monitoring
Metering
(Node Wide Part)

Compute (IaaS)

Storage SDS

Network SDN

Node Wide
Identity Access
Management

Container layer (K8s aaS)

Cater to the Infra-as-Code use case

- Full control over kubernetes (k8s) cluster for customer („unmanaged“)
- K8s aaS: One or several k8s cluster(s) per tenant, self-service deployment (k8s cluster API)
- Standardized across SCS providers

Tooling included (also standardized)

- Storage/Network (CSI/CNI), mesh & ingress, application deployment automation
- Repository & Security Scanning
- Monitoring & Tracing tools

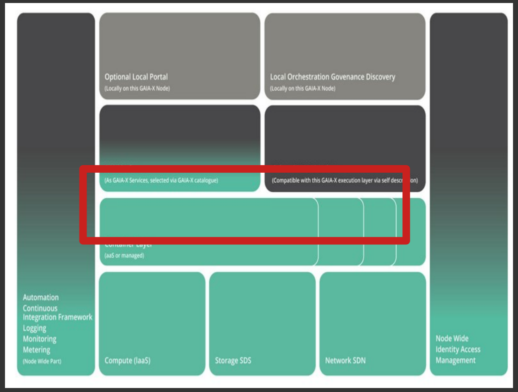
Approach reusable for providing managed clusters for customer containers

- Shared clusters are a challenge though (investigating µ-VMs/kata/firecracker)

Operator managed shared cluster for higher-level services (PaaS and SaaS)

Status: k8s cluster API adoption & maturity needs work => not standardizable yet
Working with partners & upstream to move forward.

Fill the gap: PoCs with SAP Gardener, Kubermatic, Rancher (rke) => GitHub.
More underway. Potentially use OpenStack k8s cluster API provider meanwhile.


Optional Local Portal
(Locally on this GAIA-X Node)
Local Orchestration Governance Discovery
(Locally on this GAIA-X Node)
(As GAIA-X Services, selected via GAIA-X catalogue)
(Compatible with this GAIA-X execution layer via self description)
Container Layer
(aaS or managed)
Automation
Continuous
Integration Framework
Logging
Monitoring
Metering
(Node Wide Part)
Compute (IaaS)
Storage SDS
Network SDN
Node Wide
Identity Access
Management

Infra & IaaS

Avoid K8s aaS on naked hardware

- Multitenancy & Isolation challenge
- Hardware management, automation, metering challenge

IaaS

- OpenStack core services (keystone, nova, neutron, cinder, glance) plus a few (ironic, barbican, octavia, telemetry)
- Containerized for easy life cycle management (kolla-ansible)
- Basically what‘s needed for K8s aaS
- Exposure to end customers optional (but standardized)

Storage

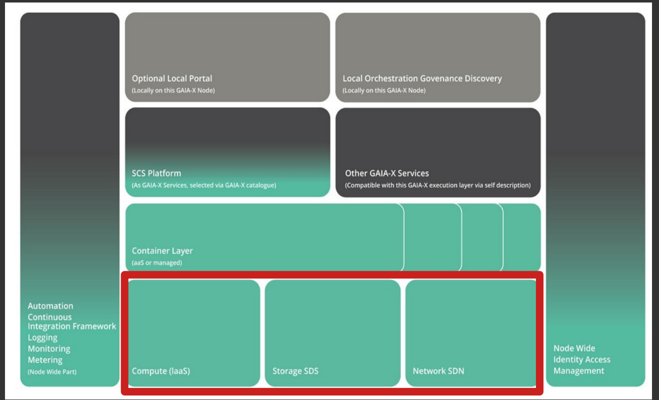
- Ceph, containerized (ceph-ansible), encrypted data at rest
- Providing block storage and object storage (s3 = standard, swift optional)

Networking

- OvS / OVN

Status

- Working (Exposure needed due to lack of standardization for k8s aaS layer)



Optional Local Portal
(Locally on this GAIA-X Node)

Local Orchestration Govenance Discovery
(Locally on this GAIA-X Node)

SCS Platform
(As GAIA-X Services, selected via GAIA-X catalogue)

Other GAIA-X Services
(Compatible with this GAIA-X execution layer via self description)

Container Layer
(aaS or managed)

Automation
Continuous
Integration Framework
Logging
Monitoring
Metering
(Node Wide Part)

Compute (IaaS)

Storage SDS

Network SDN

Node Wide
Identity Access
Management

Ops, Tooling, IAM, CI/CD

Operator focus

- Complete toolset & best practices, all openly shared
- Daily automated deployment/update with CI (more coverage WIP)
- Logging (ELK), Monitoring (netdata, skydive, prometheus/cortex, grafana), Alerting

Identity & Access Management (IAM)

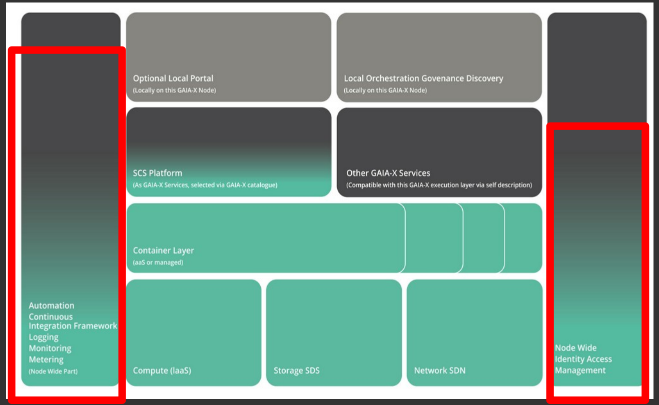
- Admin/Service account policies, 2FA (via UCS/keycloak)
- Tenants can use federation (oID connect, SAML), sharing IDs across clouds

Certification (TBD)

- SCS certification guarantees standards compliance (InterOp), quality, security
- Prepare security certifications (TC, BSI, …)
- GAIA-X self-descriptions

Status

- Deployment automation, CI, Monitoring, Logging working
- IAM: Working for IaaS (keystone), testbed implementation for addtl. keycloak
- Auditing & tracing TBD (conftest, OPA, … WIP)



Optional Local Portal
(Locally on this GAIA-X Node)

Local Orchestration Governance Discovery
(Locally on this GAIA-X Node)

SCS Platform
(As GAIA-X Services, selected via GAIA-X catalogue)

Other GAIA-X Services
(Compatible with this GAIA-X execution layer via self description)

Container Layer
(aaS or managed)

Automation
Continuous Integration Framework
Logging
Monitoring
Metering
(Node Wide Part)

Compute (IaaS)

Storage SDS

Network SDN

Node Wide
Identity Access
Management

SCS Summary

GAIA-X and SCS buildx a network of providers of interoperable, federated services (not: one European hyperscaler).

SCS helps GAIA-X node providers to easily deliver modern interoperable, federated infrastructure.

It does so by defining certifiable standards, delivering a modular open source implementation and building a provider ecosystem in which we share the tools and best practices for operating it.

SCS status: Automated deployment for Infra, Ops Tools, IaaS in daily use (CI) and in production (Betacloud). K8s aaS not yet standardizable, automation available for Gardener, Kubermatic, Rancher.

We have challenges with k8s cluster management standardization.

Nice traction in industry, CSPs and public sector.

Sovereign
Cloud Stack

Join us!

Questions?

https://scs.community/
Contact: project@scs.sovereignit.de
scs@garloff.de

Sovereign Cloud Stack

Legal Remark:

SCS, Sovereign Cloud Stack are protected trademarks of OSB Alliance e.V.
The logo is protected as well.
Other trademarks are registered trademarks of their respective owners.
No warranty for the correctness of information provided in these slides can be taken. Use at your own risk.